# Ensuring digital payment security

# PAYMENT

POSTED ON 11.26.21

Digital payments are a quick, secure, and easy way to purchase products or services, both online and in-store. To drive further adoption of digital payment cards, building consumer trust in digital payment security is paramount. Concerns about fraud and security techniques remain strong—there's still a need for reassurance. How? By simply educating consumers on the various technologies that are securing digital payments. In doing so, banks and merchants can encourage more customers to benefit from the convenience of a complete digital payment experience.

## Addressing security concerns

How secure are digital payment cards? Highly. And yet, phishing, card information theft, scams, and payment fraud remain top concerns.

As digital payments achieve rapid growth, consumers are also becoming more apprehensive of fraudulent activities. According to a survey conducted by IDEMIA and PYMNTS, **worry about fraud is the strongest inhibitor**. More than a third of people (35%) without digital payment cards said the most important reason they do not want them is because of concerns about their security. The apprehension is quite similar for online payments and in-store payments, regardless of consumer age.

Ensuring digital payment security—and letting it known to the public—is a necessity for banks to **develop customer trust, maintain loyalty, and drive market penetration**. How can they do so? Through education about authentication technologies put in place to secure payments. As the knowledge about their level of trust rises, so will their usage.

## In digital payment security we (should) trust

The paradox in all of this is that digital payments have never been as secure as they are today. Several technologies (passwords, **tokenization**, strong customer authentication, digital ID, and **biometrics**) can limit risks for sensitive data to be intercepted and used for fraudulent purposes. These complementary techniques not only **impede fraud and secure payments**; they also **maintain the speed and convenience** customers love about digital shopping. Thus, helping issuers and merchants invest in these new approaches will mitigate fraud and create market traction by allowing lightning-speed payments.

Security and customer-proven usability must be provided for easy digital onboarding, card activation and digital payments. The following **three steps** ensure both safety and a superior user experience. The outcome? Securing the journey across all channels and touchpoints, and a state-of-the-art payment experience.

## #1. Digital onboarding and identity verification

Digital payment security needs to be ensured from end-to-end, throughout the customer journey. It starts from the very beginning: the onboarding—especially when done remotely. A reliable digital onboarding process requires **layered identity proofing** including identity document and biometric verification, and even verification through third-party databases to check further attributes. This approach can be adapted according to the customer profile, the financial institution's risk policies, and the level of requirements from local regulations.

A quick, convenient and secure **customer digital onboarding can be processed directly with a mobile phone**. It's as easy as taking a picture! The customer starts the ID proofing process by first downloading the bank's mobile application or visiting their website. From there, they only need to scan their identity document using the camera of their smartphone and take a selfie to submit it for biometric verification against the photo on the document provided. These pieces of evidence are verified, and background checks (identity verification against official sources such as a Root of Trust, comparison with criminal databases, etc.) can also be quickly performed. Once the application is approved, the digital payment card is immediately issued. **This digital onboarding is as quick and convenient as it is secure**.

The digital onboarding process **protects both the card issuer and consumers**, who now know that their ID and financial activities are strongly protected. They can now apply for a card digitally and receive it in real time for immediate, secure, payments—online and in-store!

## #2. Tokenization, the cornerstone of digital payment security

Tokenization has become the best, most-secure way to address a great variety of use cases regarding identity proofing or payments. The principle is simple:

- The real card data is replaced by a non-sensitive, **randomly generated equivalent**—a token. There is no mathematical relationship between this token and the real data it represents; no key can "reverse them" back to the actual information.
- Tokenization uses a **token vault**, which stores the relationship between the sensitive value and the token, and the token itself for cloud payment use cases.

Tokenization secures all the user data, protecting the cardholder from fraud. It is a fundamental enabler of many digital payments use cases, for both physical and remote purchases.

- As you **shop in store using** your phone or connected watch to pay via Apple Pay, Google Pay, Samsung Pay or even some Issuer Pay (provided by banks that create their own digital wallet for cardholders), it is a token, not your actual card data, that is transmitted from your device to the merchant.
- For **online payments**, other use cases are enabled, including one-off payment in a guest checkout; repeat purchases and recurring payments, through buy-buttons such as Amazon 1-Click or another merchant website; and Click to Pay, the new unified pay button.

## #3. Cardholder authentication technologies

Another layer of security is brought by the **authentication of the cardholder**. Identity verification, presented above, aims to check that "I am who I claim to be" when opening an account. The purpose of authentication technologies is to verify that the payment is performed by the genuine consumer—"It's really me who is using this card now." You may have already experienced an online payment journey where you are asked to enter an OTP code received on your phone to authenticate before validating the payment. This is one way to ensure the cardholder authentication, as is the case with 3D Secure.

**Biometrics** can also play a great role in streamlining the user payment experience and to reinforce trust. Through fingerprints or selfie checks, the payer is authenticated, and the payment validated. As biometrics requires something

unique to each individual, it greatly reduces the chance of fraudulent transactions.

## Maintaining trust

The banking business is built on trust. As customers increasingly benefit from digital and mobile financial services, **they want to be assured that their personal data remains protected**. Given the vast array of devices used to access banking apps, and the diverse attack points for cyber criminals, digital payment security cannot be limited to one area; only a holistic approach can protect all the devices and all the journeys. The combination of **tokenization techniques** with **identity proofing and authentication technologies backed by biometrics** is the most efficient way to resolve potential security threats while ensuring reliability, speed, and convenience. Better **informing customers about the security measures** in place and adopting this holistic approach will increase your customer base—it will show them that you care about keeping them safe and satisfied, and drive usage of your digital payment cards.